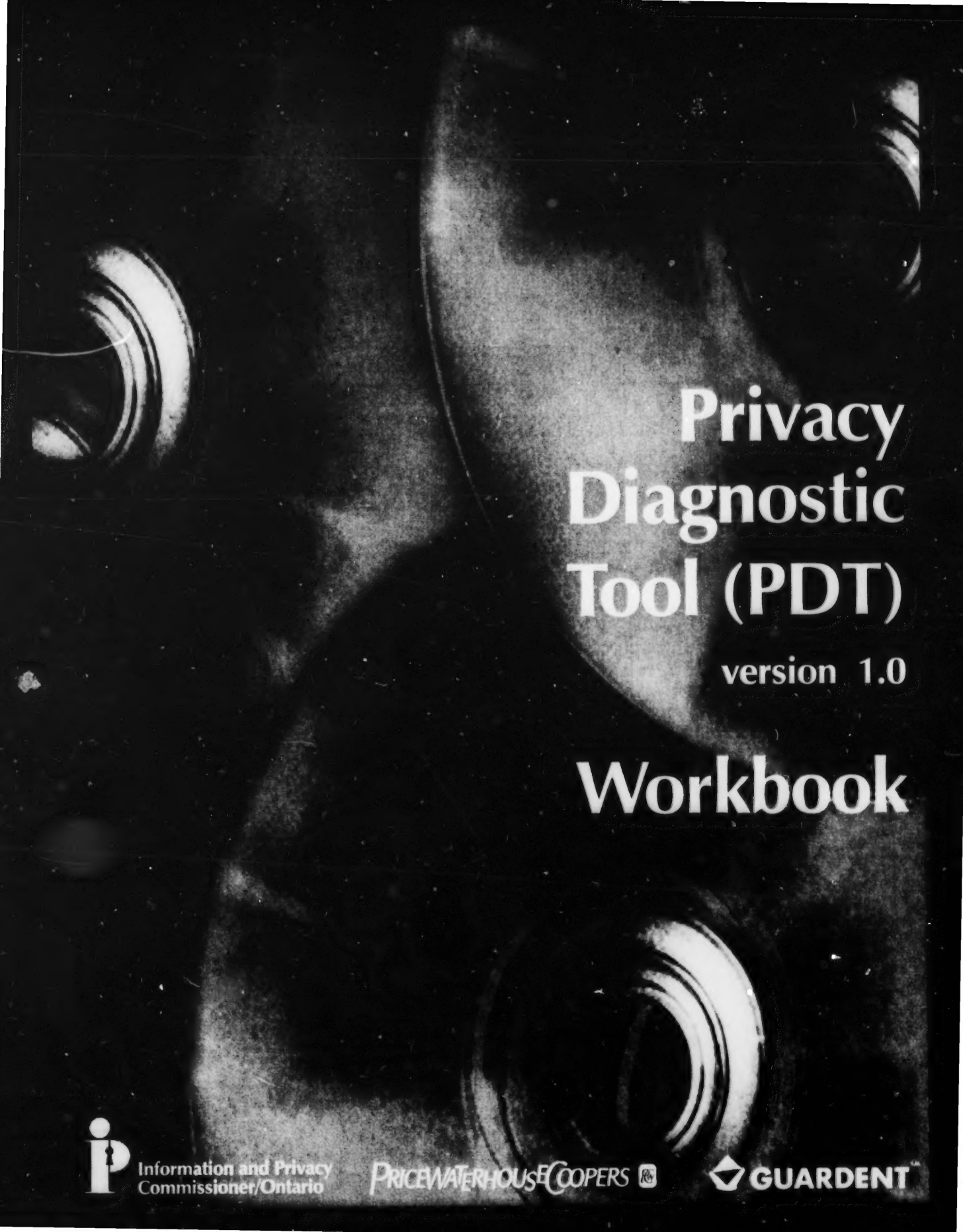
Privacy
Diagnostic
Tool (PDT)
version 1.0
Workbook
Information and Privacy
Commissioner/Ontario
PRICEWATERHOUSECOOPERS
GUARDENT

This workbook and the Privacy Diagnostic Tool are available on the Web site of the Office of the Information and Privacy Commissioner/Ontario.

Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: http://www.ipc.on.ca

GUARDENT™

Guardent Canada Inc.
1 St. Clair Avenue West, 7th Floor
Toronto, Ontario M4V 1K6
416-927-8659
Fax: 416-927-7593
E-mail: john.rombough@guardent.com

PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers
Global Risk Management Solutions
145 King Street West
Toronto, Ontario M5H 1V8
416-814-5729
Fax: 416-814-5777
E-mail: michael.deck@ca.pwcglobal.com

Foreword

There is no question that a growing number of businesses are interested in learning more about privacy and how to protect their customers' personal information. Surveys show this to be the case, and the growing number of speaking requests that my office has been receiving from the private sector clearly supports that fact. Over the past year in particular, I have found that after every speech or presentation I deliver, business people have approached me to ask: *Where do I start?*, *How do I begin protecting my customers' information?* and *What tools are available to assist me?* Unfortunately, there have been very few places for me to point them to, and few helpful tools to offer them.

Faced with this frustration, it struck me that what was needed was a simple, plain language tool, based on questions and answers for businesses looking for help and direction in implementing privacy at a concrete level. Those businesses need assistance, not only in determining what their state of privacy readiness is, but also what steps to take to identify and address what is missing.

This prompted me to do two things: first, to attempt to fill the void by developing some kind of privacy diagnostic tool and second, to seek out help from those familiar with the business world, in order to ensure that the tool would be both relevant and responsive. I approached Guardent and PricewaterhouseCoopers to participate in a project with my office. To my delight, both graciously agreed to work with us in developing the Privacy Diagnostic Tool (PDT) that you now have before you. Their business expertise was invaluable and, coupled with the privacy expertise of my office, lead to the development of this new, easy-to-use tool for businesses.

I would like to extend my sincere thanks to Guardent and PricewaterhouseCoopers for working with us to produce what I believe is an excellent tool. I trust that you will find this tool valuable in meeting the challenges of implementing privacy in a rapidly changing, information-driven economy, and wish you every success.

Ann Cavoukian, Ph.D.
Commissioner

Table of Contents

Introduction 1

Principle 1 — Accountability 5

Principle 2 — Identifying Purposes 8

Principle 3 — Consent 11

Principle 4 — Limiting Collection 14

Principle 5 — Limiting Use, Disclosure, and Retention 17

Principle 6 — Accuracy 21

Principle 7 — Safeguards 23

Principle 8 — Openness 27

Principle 9 — Individual Access 30

Principle 10 — Challenging Compliance 33

Glossary of Terms 35

Related Privacy Links 39

Introduction

In January 2000, the *Wall Street Journal* published a survey that showed privacy as the number one concern for North Americans for the 21st century. More recently, on March 5, 2001, Forrester Research completed a study of privacy issues for business. They stated that, "Anyone today who thinks the privacy issue has peaked is greatly mistaken ... we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope."

At the same time, advances in information technology and the Internet have changed the way that companies do business. Over the past decade, we have seen unparalleled growth in the ability of organizations to collect, compile, analyze, and disseminate personal information, not to mention the unprecedented volume of personal information that organizations routinely collect. As the *Wall Street Journal* and others attest, consumers expect their personal information to be protected and their privacy to be respected by the organizations they do business with. Breaching consumer expectations or breaking their trust lands organizations on the wrong side of the privacy issue.

Today, leading businesses recognize that privacy concerns threaten the bottom line. Accordingly, addressing privacy concerns effectively is beginning to be seen as a winning strategy for both business and consumers.

What is Privacy and Why Does It Matter?

A wide variety of interrelated values, rights, and interests come together under the rubric of privacy. For most businesses, however, the most relevant sub-set of privacy is informational privacy (also known as data protection).

Information privacy is the ability of an individual to exercise a substantial degree of control over the collection, use, and disclosure of their personal information.

Personal information includes any information about an identifiable individual. This includes information such as name, address, gender, age, ID numbers, income, ethnic origin, employee files, credit records or medical records. An individual's name need not be attached to the information in order for it to qualify as personal information.

Most companies need to collect, use and disclose some information about their customers in order to conduct their business. But organizations must be reasonable and fair in their treatment of personal information, not only for the good of their customers, but also for the good of their own business reputations. Consumers are no longer willing to overlook a company's failure to protect their privacy. High profile misuses of personal information have shown that a lack of respect for personal information can bring both harsh criticisms from consumers, and significant devaluation of company shares.

Thanks in part to much publicized incidents, many jurisdictions have seen a wave of legislative initiatives, such as the European Union Directive on Data Protection and Canada's *Personal Information Protection and Electronic Documents Act*. Organizations around the world are now beginning to take note of international and local regulatory initiatives that may influence how they treat customer information.

There is no better time than the present for organizations that handle personal information to take a close look at their practices and bring them into line with emerging consumer expectations. In the short term, protecting personal information and developing consumer trust promise to become a strong competitive advantage. In the long term, protecting privacy will become a new business imperative.

The Privacy Diagnostic Tool (PDT): What's In It For Me?

Organizations interested in doing business must take data privacy issues very seriously. According to a Senior Executive Panel at the May 2001, *Computerworld* Premier 100 Conference, even one privacy slip-up could be devastating to a company's corporate image and brand.

Can an organization benefit from paying attention to the PDT and taking the time to use it? To help you and your organization decide whether or not to use the PDT, please review the following questions. If your organization answers yes to one or more of these questions, you will benefit from using the PDT. In fact, we highly recommend it.

Questions

1. Does your organization collect and use personal information in the course of your business?
2. Is the use of personal information an important part of your business (for example, as part of marketing, sales or Customer Relationship Management)?
3. Do you disclose your customer's information to anyone?
4. Have you bought, sold, traded or shared personal information?
5. Is your organization potentially vulnerable to internal or external security breaches involving your customers' personal information?
6. Do you have any questions on how current or upcoming privacy regulations will affect the way you collect and use personal information?

If you answered yes to one or more of the above questions, you will benefit from using this Privacy Diagnostic Tool.

Using the Privacy Diagnostic Tool

The PDT is a voluntary, self-administered assessment of whether and to what extent your business's information management practices are privacy-friendly. Working through a series of questions, the PDT will help you to both assess and educate your organization, ensuring a better understanding of how to protect personal information and build consumer trust.

The PDT addresses ten principles that are key to the proper management of personal information, based on internationally recognized norms known as Fair Information Practices (FIPs). FIPs are overlapping and cumulative principles that outline responsible information handling practices. They cover the following areas:

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

The PDT outlines each principle, explains its objectives, and notes some risks that your organization may face if it fails to adhere to the principle.

For each principle, there is a series of questions on implementation, divided into two sections. The first section, *Implementing the Principles*, identifies and assesses your compliance with the *required* steps for implementing the principle. The second section, *Best Practices*, identifies and assesses your compliance with *best practices* for implementing the principle. Simply answer *Yes* or *No* to each question, based upon your current business practices. If the requirement or best practice is not applicable to your organization, answer *Yes*.

If you have answered *No* to one of the questions under the heading *What You Need to Do*, your organization is not fully adhering to that Fair Information Practice. You should review and amend your policies and procedures to ensure a *Yes* response. If you answered *No* to any of the *best practices*, consider whether you should adopt this practice in your organization.

About the Privacy Diagnostic Tool

Please note that this tool is not designed to provide a detailed privacy audit or an in-depth privacy impact analysis. Use of this tool should be viewed as an initial gauge of one's privacy readiness – it is intended to be complimentary to other measures you might take to protect privacy and to any measures you may be required to take for compliance with privacy legislation and other legal standards or industry privacy codes applicable to your organization.

We have endeavoured to make this tool as useful as possible. However, the Information and Privacy Commissioner/Ontario (IPC) takes no legal responsibility for the results of using this tool. The information contained in this publication should not be considered legal, accounting, tax or other professional advice or services. (If you need specific advice about your particular situation, you should always consult a suitably qualified professional.)

The PDT has been developed by the IPC with the generous assistance of Guardent and PricewaterhouseCoopers. Any errors or omissions are the sole responsibility of the IPC.

The PDT is available free of charge to any company that wishes to examine its information management policies, or to consumers who may want a tool to analyze the privacy practices of the businesses with which they interact. It is also designed to be completed anonymously and does not require the provision of results or information to any of the developers.

System Requirements

The PDT is available in three formats:

Systems running Microsoft Access 2000

- Pentium-based personal computer
- Microsoft Windows 95/98/2000/NT
- Microsoft Access 2000
- 64 MB of RAM
- 3 MB of disk space
- CD-ROM drive

Systems running Microsoft Access 97

- Pentium-based personal computer
- Microsoft Windows 95/98/2000/NT
- Microsoft Access 97
- 64 MB of RAM
- 3 MB of disk space
- CD-ROM drive

Systems not running Microsoft Access

- Pentium-based personal computer
- Microsoft Windows 95/98/2000/NT
- 64 MB of RAM
- 50 MB of disk space
- CD-ROM drive

Principle 1 Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with established privacy principles.

Objectives

This principle focuses on identifying and assigning ultimate responsibility for compliance. Appropriate accountability will ensure effective implementation, policy development, adherence, evaluation and refinement of privacy protection throughout your organization.

Your privacy policies and practices need to apply to **all** personal information in your control. Information in your control includes not only the data in your physical custody, but also personal information you may have transferred to a third party, such as a contractor, for data processing.

Potential Risk

- Unclear accountability could lead to mismanaging customer information (e.g., breaching customer trust, inappropriately disclosing personal information), which could damage to your reputation and business relationships.
- Unclear accountability will make it more difficult for you to respond to customer complaints effectively, leading to customer dissatisfaction and potential loss of business.
- Unclear accountability will negatively affect a meaningful review of your company's information management practices.

Implementing the Principle

What You Need To Do

- You assign accountability for compliance with these principles to a specific person or group of people in your company.

☐ Yes ☐ No

- You make available the identity and contact information of the person or group of people in your organization who are accountable for compliance with established privacy principles.

☐ Yes ☐ No

- You develop and then implement specific privacy policies and procedures.

☐ Yes ☐ No

- You use contracts and/or other measures to ensure that when third parties process personal information on your behalf, they maintain a level of privacy protection comparable to your own practices.

☐ Yes ☐ No

- You have established a complaint process to receive and respond to complaints and inquiries about your information management practices.

☐ Yes ☐ No

- You train your staff and ensure that they understand, and are capable of implementing your privacy policies and practices.

☐ Yes ☐ No

Best Practices

- You regularly review your privacy policies and practices with staff to ensure consistent implementation.

  ☐ Yes ☐ No

- You have a written policy in place outlining your responsibility for personal information.

  ☐ Yes ☐ No

- Front-line staff are trained to handle customer inquiries regarding:
  - privacy complaints;
  - correction requests; and
  - requests for access to personal information.

  ☐ Yes ☐ No

- You have built an ongoing compliance monitoring system.

  ☐ Yes ☐ No

- You have integrated your information management policies and practices into new staff training.

  ☐ Yes ☐ No

- You clearly mandate the responsibilities of individual staff and have regular reviews.

  ☐ Yes ☐ No

- You have specific audit and enforcement mechanisms (e.g., contracts) to ensure appropriate collection, use, and disclosure of personal information transferred to third parties.

  ☐ Yes ☐ No

- Effective compliance with privacy principles is part of the performance evaluation for individuals who have been designated as accountable for the organization's privacy policies.

  ☐ Yes ☐ No

Principle 2 Identifying Purposes

The purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Objectives

Identifying the purposes for which you need personal information to conduct your business is a critical first step in defining what personal information you need to collect, use and disclose. Your purposes should be reasonable in the context of your business. In addition, you must ensure that you do not define your purposes so broadly as to make them meaningless to the individual from whom you want to collect personal information.

In defining your purposes, consider the following actions:

- **collection** – what personal information you gather, acquire, or obtain from any source, including third parties, by any means, and why;
- **use** – how you handle and use personal information within your company; and
- **disclosure** – when, how, and why you make personal information available to third parties outside your company.

Potential Risk

- Collecting more information than you need may expose your organization to greater liability and security risk.
- Failure to design processes that match the business need to collect certain personal information could lead to the inadvertent collection of unintended information, creating additional administration costs.
- Failure to inform customers of your purpose for collecting their information may cause you to lose customers.
- Failure to identify your purposes for collecting personal information will make it difficult to responsibly manage the information in your custody.

Implementing the Principle

What You Need To Do

- You identify the legitimate purposes for collecting personal information at or before the time you actually collect the information.

  ☐ Yes ☐ No

- You define what personal information is necessary to fulfill the purposes identified, taking into account both primary and secondary purposes (e.g., audit, marketing, etc.).

  ☐ Yes ☐ No

- You document your purposes so that your staff and the individuals to whom the information relates understand these purposes.

  ☐ Yes ☐ No

- When you want to use personal information already in your custody for a new purpose **not** identified at the time of the initial collection, you seek the consent of the individual, unless the new purpose is required by law.

  ☐ Yes ☐ No

- You have examined opportunities for using non-identifiable information (i.e., coded, anonymous, pseudonymous, or aggregated data) rather than personal information to meet your purposes.

  ☐ Yes ☐ No

Best Practices

- Your identified purposes for collecting personal information are publicly available at the time of collection.

  ☐ Yes ☐ No

- Employees collecting personal information are able to explain to individuals the purposes for which the information is being collected.

  ☐ Yes ☐ No

- You have clear procedures in place to seek informed customer consent prior to using or disclosing personal information for new purposes not identified at the time of collection.

  ☐ Yes ☐ No

- You review the purposes for which you collect personal information regularly, to ensure that they remain current.

  ☐ Yes ☐ No

- The identified purposes for collecting personal information are communicated to the business areas responsible for processing and collecting the data.

  ☐ Yes ☐ No

- Staff pro-actively explain to customers what personal information is collected and why.

  ☐ Yes ☐ No

Principle 3 Consent

The knowledge and informed consent of the individual are required for the collection, use, or disclosure of personal information, except where exempted by law.

Objectives

This principle places an explicit obligation on you to obtain consent from individuals for the collection, use and disclosure of their data, except in limited circumstances.

This principle requires both knowledge **and** consent. This means that you should not ask for consent unless you have made a reasonable effort to inform individuals of the purposes for which you will be collecting, using and disclosing their personal information. In addition, you should not use consent to attempt to override your obligations and responsibilities under these principles.

Consent is a voluntary agreement with what is being done or proposed. Consent can be obtained in a variety of ways, and may include both explicit and implied forms of consent. You should consider the sensitivity of the personal information involved when determining what method is appropriate. As a general rule, the greater the potential harm to individuals if their personal information is misused, the greater your responsibility to ensure that their consent is informed and explicit.

Potential Risk

- Failure to seek consent or seeking consent in ways not appropriate to the sensitivity of the information could erode customer trust and may result in a backlash; this in turn may result in loss of reputation.
- Failure to obtain consent may decrease the efficacy of some business practices, such as marketing, by targeting products and services to uninterested parties.
- Failure to obtain consent will result in legal liabilities or sanctions where the obligation to seek consent is required by law or self-regulation.
- Failure to get explicit consent may contribute to customers withdrawing their consent for future information use.

Implementing the Principle

What You Need to Do

- Consent is obtained for the collection, use and disclosure of personal information, at or before the time of collection, except where not appropriate (e.g., exchange of information with credit agency for a loan).

  ☐ Yes ☐ No

- You take into account the sensitivity of the personal information when determining what form of consent is appropriate for the circumstances (e.g., express or implied consent; opt-in or opt-out).

  ☐ Yes ☐ No

- You make a reasonable effort to advise the individual of the purposes for which the information will be used.

  ☐ Yes ☐ No

- You do **not** make consent to the collection, use or disclosure of personal information for secondary purposes, such as marketing, a condition of the supply of your product or service.

  ☐ Yes ☐ No

- You do **not** deceive or mislead the individual in order to obtain consent.

  ☐ Yes ☐ No

- You inform individuals that they may withdraw consent at any time, and explain the implications of their withdrawal to them.

  ☐ Yes ☐ No

Best Practices

- You take into account the reasonable expectations of the individual when determining how to seek consent; for example, positive, express consent is sought where the information is sensitive.

  ☐ Yes ☐ No

- You periodically review and update consent and withdrawal of consent for each individual.

  ☐ Yes ☐ No

- You document the mechanism by which consent is given (e.g., over the telephone, in writing, by e-mail, etc.).

  ☐ Yes ☐ No

- You verify when, and for what reasons, consent for the collection of personal information has not been obtained from an individual.

  ☐ Yes ☐ No

- You review your staff's actions in obtaining customer consent and advising customers of their options.

  ☐ Yes ☐ No

- You regularly review the customer consent process.

  ☐ Yes ☐ No

- You have processes in place that ensure consent is gained before personal information is disclosed within or outside your organization.

  ☐ Yes ☐ No

Principle 4 Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Objectives

This principle limits the amount and type of personal information you may collect from any source, including third parties.

You must be able to establish a clear link between the information you collect and the purposes you have identified for collecting information. This principle requires you not to collect personal information beyond that which is necessary to fulfil your identified purposes.

Potential Risk

- Failure to limit your collection of personal information increases the volume of data you are responsible for managing, and may expose your organization to increased costs and greater liability.
- The more information you collect, the greater the chances of inaccuracy.
- Unfair or unlawful collection may expose you to charges of deceptive business practices.
- Collecting more information than is necessary for your purposes may aggravate your customers, resulting in lost business.
- If your organization collects information electronically (e.g., cookies), failure to inform your customers could lead to a backlash against your organization.

Implementing the Principle

What You Need to Do

- You limit both the type and amount of personal information you collect to only that which is necessary for your identified purpose(s).

  ☐ Yes ☐ No

- You collect personal information in a fair and lawful way, and do not deceive or mislead individuals.

  ☐ Yes ☐ No

- You do **not** collect personal information indiscriminately.

  ☐ Yes ☐ No

- You describe what type of personal information you collect and how it will be used and disclosed.

  ☐ Yes ☐ No

Best Practices

- You communicate your collection practices clearly, avoiding highly subjective or ambiguous phrasing that may confuse customers.

  ☐ Yes ☐ No

- You restrict the amount and type of information you collect to that which the individual has consented to.

  ☐ Yes ☐ No

- You inform customers of their options to restrict the collection of their personal information, where available.

  ☐ Yes ☐ No

- You seek or have sought customer feedback regarding the clarity and comprehension of your collection practices.

  ☐ Yes ☐ No

- There is a regular review of information collection and handling practices to ensure compliance with the restricted collection principle.

  ☐ Yes ☐ No

- If you collect personal information from a third party, you ensure the third party has gained consent from the customer for the disclosure.

  ☐ Yes ☐ No

- Your organization uses opt-in consent prior to using cookies or any other information collected electronically.

  ☐ Yes ☐ No

Principle 5 Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the informed consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Objectives

You should use or disclose personal information only for the purposes identified to the individual at the time of collection. New uses or disclosures are permissible only with the consent of the individual or as required by law.

This principle imposes a responsibility on you to keep personal information for a minimum length of time; either as specified in industry standards or applicable legislation or only as long as it is needed to achieve the identified purposes.

Potential Risk

- Use or disclosure of personal information beyond your identified purposes jeopardizes customer trust and may give rise to charges of deceptive business practices.
- Without a defined retention schedule, you run the risk of either retaining information for too long, thereby incurring additional information management costs, or destroying information prematurely, thereby eroding the ability of individuals to access information about themselves, and eroding your potential use of needed information.

Implementing the Principle

What You Need to Do

- You use and disclose personal information in your control only for the purposes for which you collected it, unless you have obtained consent, or the use or disclosure are required by law.

☐ Yes ☐ No

- You document your use of personal information for any new purpose(s) not initially communicated to customers when receiving their consent.

☐ Yes ☐ No

- You retain information only as long as necessary to fulfil your identified purposes (you have a policy of purging personal information from your databases).

☐ Yes ☐ No

- You retain personal information used to make a decision about an individual long enough to allow the individual to access that data and challenge its accuracy.

☐ Yes ☐ No

- You have procedures in place to govern the secure destruction of personal information.

☐ Yes ☐ No

Best Practices

- You only use and disclose personal information for purposes identified at the time of collection.

  ☐ Yes ☐ No

- You have defined limited and specific exceptions for when you will use or disclose information for reasons other than those identified at the time of collection.

  ☐ Yes ☐ No

- You have both policy and technical restraints in place to limit your use and disclosure of personal information to your identified purposes.

  ☐ Yes ☐ No

- You communicate the limitations on use and disclosure of personal information to all pertinent staff.

  ☐ Yes ☐ No

- You monitor your procedures, legal contracts, policies, and technical controls regularly to ensure appropriate restrictions on the use and disclosure of personal information are in place.

  ☐ Yes ☐ No

- You disclose personal information to third parties only for purposes identified at the time of collection.

  ☐ Yes ☐ No

- Your data retention practices include specific retention procedures, as well as minimum and maximum retention periods.

  ☐ Yes ☐ No

- You have a clear timetable for retaining and disposing of personal information.

  ☐ Yes ☐ No

- You communicate your practices regarding use, disclosure, and retention, to the business functions responsible for retaining personal information.

  ☐ Yes ☐ No

- You retain personal information only for the purposes for which you have collected it, except when required by law.

  ☐ Yes ☐ No

- Personal information that is no longer required to fulfill the identified purposes is destroyed, erased, or rendered anonymous.

  ☐ Yes ☐ No

- You inform individuals of your retention periods and what you intend to do with the information after the maximum retention periods are reached.

  ☐ Yes ☐ No

- You update personal information only as appropriate.

  ☐ Yes ☐ No

Principle 6 Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Objectives

Your business need for accurate personal information will vary according to the purposes for which you collect, use, and disclose it.

As a general rule, if you use or disclose personal information on an on-going basis, you should make sure it is accurate. For some purposes, however, you may not require information that is current and up to date. In these cases, you should limit your efforts to update personal information to only what is necessary.

When determining the necessary degree of accuracy, completeness and timeliness of data, you need to consider the requirements of your identified purpose and whether the individual might be harmed by your use or disclosure of inaccurate information.

Potential Risk

- Use of inaccurate information to make decisions about customers can lead to lost profits and market share.
- Inaccurate information may harm the customer, and jeopardize customer relations.
- Failure to identify inaccurate information may lead to business decisions being made on the basis of incorrect, and possibly misleading, information.
- Failure to identify the appropriate need for current and up to date information may lead to unnecessary updates, resulting in wasted resources and customer annoyance.

Implementing the Principle

What You Need to Do

- You keep the personal information in your control only as accurate, complete and up-to-date as necessary for the identified purposes.

☐ Yes ☐ No

- You take into account the interests of the individual when determining how accurate, complete and up-to-date personal information in your custody needs to be.

☐ Yes ☐ No

- You ensure that personal information is sufficiently accurate to minimize the chances of inappropriate data being used when making decisions about individuals.

☐ Yes ☐ No

Best Practices

- Your practice defines when updates are appropriate, based on your purposes and the interests of your customers.

☐ Yes ☐ No

- Any limits to the requirement for accuracy are clearly set out.

☐ Yes ☐ No

- You have procedures to verify and correct personal information.

☐ Yes ☐ No

- You inform individuals of how to access and correct the personal information in your custody.

☐ Yes ☐ No

- You conduct periodic assessments of accuracy in your databases.

☐ Yes ☐ No

Principle 7 Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Objectives

Your security safeguards, both electronic and physical, should be appropriate and proportional to the sensitivity of the personal information involved. The more sensitive personal information is, the more security is required.

While some types of personal information (e.g., medical or financial data) are generally considered sensitive, other types of information may be sensitive depending upon the context.

In determining the level of sensitivity, consider how much personal information could be revealed if accessed by unauthorized parties, as well as the potential harm to the individual if the data is misused or disclosed in an unauthorized manner. The greater the potential harm, the greater your security requirement.

Potential Risk

- Without appropriate security measures, unauthorized parties (both within and outside your company) may be able to access, use, copy, disclose, alter, and destroy the personal information in your custody, which you are responsible for protecting. Such action could create significant harm to the individual to whom the data relates, as well as potential liability for your company.
- Without appropriate access control mechanisms, unauthorized individuals may access personal information for unauthorized purposes.
- Without appropriate audit trails for access to personal information, security breaches may not be detected and remedied.

Implementing the Principle

What You Need to Do

- You implement security safeguards to protect personal information in your control against loss or theft, and unauthorized access, disclosure, copying, use, or modification.

  ☐ Yes ☐ No

- Your security safeguards are appropriate and proportional to the sensitivity of the personal information in your custody.

  ☐ Yes ☐ No

- You protect all personal information in your control, regardless of its format.

  ☐ Yes ☐ No

- You make your staff aware of the importance of maintaining the confidentiality of personal information in your control.

  ☐ Yes ☐ No

- You dispose of or destroy personal information in a way that prevents unauthorized parties from gaining access to it.

  ☐ Yes ☐ No

Best Practices

- Your premises are conducive to keeping client/employee information private and confidential.

  ☐ Yes ☐ No

- Third party monitoring and audit of security systems are conducted on a regular basis.

  ☐ Yes ☐ No

- You communicate your security safeguards regarding access, use, disclosure, and disposal of personal information to all relevant staff.

  ☐ Yes ☐ No

- You document misuses of personal information and notify affected customers.

  ☐ Yes ☐ No

- You have an information security policy that includes specific requirements for the identification and authorization of personnel with access to personal information.

  ☐ Yes ☐ No

- All personnel have unique identifiers, which are used to access personal information.

  ☐ Yes ☐ No

- All personnel are authenticated (for example, by the use of a password) in order to gain access to personal information, using an authentication mechanism commensurate with the scope of access, and the sensitivity of the information.

  ☐ Yes ☐ No

- You have an information security policy that includes specific requirements for maintaining the confidentiality of personal information.

  ☐ Yes ☐ No

- You transmit personal information over secure channels and/or encrypt any transmissions over open channels.

  ☐ Yes ☐ No

- You physically secure paper records containing personal information.

  ☐ Yes ☐ No

- You have an information security policy which includes specific requirements for the creation of audit trails for all information systems that process personal information and for the active monitoring of all information systems that process personal information.

  ☐ Yes ☐ No

- Intrusion detection systems (host or network based) are implemented for all information systems that contain personal information.

  ☐ Yes ☐ No

- Procedures have been defined for the monitoring of intrusion detection systems, and for responding to any alerts that are generated.

  ☐ Yes ☐ No

Principle 8 Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Objectives

This principle places an obligation on you to be open and transparent in your information management practices. In doing so, this principle ensures that your accountability for personal information is effectively implemented and that individuals can obtain the information they need in order to make informed decisions about their business relationship with you. Openness and transparency are essential components of customer trust.

The information you make available about your policies and practices must include the name (or title) and address of the person who is accountable for them, and to whom individuals may direct their complaints or inquiries.

In addition you must make available a description of the following:

- how individuals can get access to personal information in your control;
- the type of personal information you hold;
- how you use personal information; and
- what personal information you make available to related organizations.

Finally, you must make publicly available a copy of any brochures or other documented information explaining your privacy and information management policies, practices, standards, or codes.

Potential Risk

- Inaccessibility to an organization's privacy program prevents individuals from gaining an understanding of how an organization handles and protects their personal information, and may undermine the ability to obtain informed consent.
- Without openness you sacrifice customer trust and confidence and undermine your customer relations management.

Implementing the Principle

What You Need to Do

- You are open about your policies and practices with respect to the management of personal information.

☐ Yes ☐ No

- You make available details on the type of personal information you hold, how it is used and disclosed, and how to access it.

☐ Yes ☐ No

- You enable individuals to obtain information about your policies and practices without an unreasonable effort.

☐ Yes ☐ No

- You make that information available in a format that is generally understandable.

☐ Yes ☐ No

Best Practices

- You make information on your policies and practices available in a variety of ways, depending on the nature of your business (e.g., through brochures, online access, or a toll-free telephone number).

  ☐ Yes ☐ No

- A description of your privacy program is included in all third party partner agreements and contracts.

  ☐ Yes ☐ No

- You explain the use of any non-visible tracking tools such as click stream data, and clear GIF files (Web Bugs).

  ☐ Yes ☐ No

- Your employees understand and commit to complying with your organization's privacy program.

  ☐ Yes ☐ No

- You communicate your compliance with your privacy policies and practices through appropriate means (e.g., professional memberships, privacy seals, publication of notices of non-compliance).

  ☐ Yes ☐ No

Principle 9 Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Objectives

In order for individuals to be able to make informed decisions about their business relationship with you, and to effectively exercise some control over their personal information, they must be able to access personal information about themselves. Equally as important, they must also be able to correct inaccurate or incomplete information.

It may not always be appropriate or possible for you to provide access to all the personal information you have. Nevertheless, you have a responsibility to provide as much access as is reasonably possible. Your reasons for not allowing an individual to access their personal information should be limited, specific, reasonable, and justified. Where you are unable to provide full access, you should provide an explanation for the denial to the individual.

This principle places a responsibility on you to facilitate individuals' right of access and correction, on request.

Potential Risk

- Failure to provide customer access may result in inaccurate data.
- Failure to consider customer access in the design of information management systems may result in substantial subsequent costs.
- Ignoring a customer's right to challenge your organization's compliance will escalate privacy complaints and make them far more costly to resolve.

Implementing the Principle

What You Need to Do

- Upon request, you tell individuals if you have personal information about them and provide access to that data, except in limited circumstances.

  ☐ Yes ☐ No

- You tell individuals how their personal information is being used, and to whom it has been disclosed.

  ☐ Yes ☐ No

- You respond to an individual's request for access in a reasonable time, and at minimal, or preferably no, cost.

  ☐ Yes ☐ No

- You provide the requested information to the individual in a format that is generally understandable, along with any explanation needed to facilitate the individual's understanding.

  ☐ Yes ☐ No

- You enable the individual to challenge the accuracy and completeness of personal information in your control, and amend it as appropriate.

  ☐ Yes ☐ No

- You attach a statement of disagreement to records where you cannot agree to the requested amendment.

  ☐ Yes ☐ No

Best Practices

- You authenticate the identity of the individual making a request for personal information.

  ☐ Yes ☐ No

- You provide individuals with a list of organizations to which you may have disclosed their personal information, if you cannot give them a list of the actual disclosures.

  ☐ Yes ☐ No

- You send the corrected data, or the statement of disagreement, to third parties who have previously accessed the personal information in question, as appropriate.

  ☐ Yes ☐ No

Principle 10 Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Objectives

This principle addresses an individual's right to challenge your compliance with these privacy principles, and with your stated privacy policies and practices. It makes you responsible for enabling the individual to effectively exercise that right. The purpose is not only to enhance your accountability, but also to empower the individual.

Potential Risk

- Without an effective process to challenge compliance, individuals will be unable to evaluate your privacy program and your handling of their personal information.
- Failure to provide this component of customer service could result in customer dissatisfaction and loss of business.
- Without a process to challenge compliance, you risk losing the opportunity to improve your business practices.

Implementing the Principle

What You Need to Do

- You have procedures to receive and respond to complaints or inquiries about your handling of personal information.

  ☐ Yes ☐ No

- You explain your inquiry and complaint procedures to individuals.

  ☐ Yes ☐ No

- You investigate all complaints.

  ☐ Yes ☐ No

- You take appropriate measures to rectify the situation, if you find a complaint to be justified.

  ☐ Yes ☐ No

- You change your information management policies and practices, if necessary.

  ☐ Yes ☐ No

Best Practices

- Your compliance process is easily accessible and simple to use.

  ☐ Yes ☐ No

- Your staff responds to public enquiries in a fair, accurate and timely manner.

  ☐ Yes ☐ No

- Complaint and dispute resolution processes are regularly monitored for effectiveness, fairness, impartiality, confidentiality, ease of use, and timeliness.

  ☐ Yes ☐ No

Glossary of Terms

Access (Individual Access)

Upon request, an individual shall be informed of the existence, use, and disclosure of his/her personal information and shall be given access to that information.

An individual shall have the right to challenge the accuracy and completeness of the information and have it amended as is appropriate.

Accountability

An organization is responsible for personal information under its control and shall designate individual(s) who are accountable for the organization's compliance with the Fair Information Practice principles and applicable legislation.

Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is collected.

Personal information shall be updated only when necessary to fulfill the purposes for which it was collected.

Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual(s) accountable for the organization's compliance.

Consent

There must be voluntary agreement of the data subject to the collection, use, and disclosure of his/her personal information. This consent may be either express or implied, and should include an explanation as to the implications of withdrawing consent.

Express consent is given explicitly and unambiguously, either verbally or in writing. It is unequivocal and does not require any inference on the part of the organization seeking consent.

Implied consent is given when the action/inaction of an individual reasonably infers this consent.

Consent should never be a condition for supplying a product or service, unless the information requested is required to fulfill an explicitly specified and legitimate purpose.

Disclosure

Disclosure occurs when personal information is made available to other areas within an organization for which the information was not originally collected, or to others outside the organization.

Identify the purpose

Purposes, which include why information is being collected and how it will be used, shall be identified by the organization at or before the time of collection.

The reason for collecting information should be documented. The individual from whom the information is collected should be informed as to why this information is required.

Limiting Collection

The collection of personal information must be limited to that which is necessary for the purposes identified by the organization.

Information shall be collected by fair and lawful means. The type and amount of information collected should be limited to that which is necessary for the purposes identified.

Staff members must be able to explain the reason for collecting information.

Limiting Use, Disclosure, Retention

Personal information shall not be used or disclosed for purposes other than for which it was collected, except with the consent of the individual or as required by law.

Any new use for personal information must be identified. Consent must be obtained from an individual before the information is used for the purpose identified.

Personal information shall only be retained as long as is necessary for the fulfillment of the purposes identified. Maximum and minimum retention periods, which take into account any legal requirements or restrictions and redress mechanisms, should be instituted.

Information without a specific purpose or that no longer fulfils its intended purpose shall be disposed of in a manner that prevents improper access, such as the shredding of paper files or deletion of electronic records.

Policies outlining the type and frequency of updates to information should be established.

Openness An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals, in a manner that is easy to understand. Customers, clients, and employees shall be informed of these policies.

Personal Information Personal information is any factual or subjective information, recorded or not, regarding an identifiable individual. Examples include name, age, identification numbers, income, ethnic origin, blood type, opinions, evaluations, comments, social status, disciplinary actions, employee files, credit or loan records, medical records, or the existence of a dispute between a consumer and a merchant.

Personally Identifiable Information Personally identifiable information is any data that uniquely links an individual to other piece(s) of data. Examples include PINs (personal identification numbers), access cards, passwords, retinal and fingerprint scans, and e-mail or IP addresses. This type of information should be treated in the same manner as personal information collected in an 'offline' environment.

Privacy Privacy is the fundamental right of an individual to decide about the processing of his/her personal data as well as to protect his/her intimate sphere. Privacy violations include:

- improper acquisition of personal information, including its access, collection, and distribution;
- improper use of information, including its use for reasons other than for which it was explicitly collected or its transfer to other parties;
- unwanted solicitation of personal data; and
- improper storage of information.

Retention Period A retention period is the duration of time personal information is held. Personal information should not be held for longer than isnecessary to fulfill the purpoes for which it was collected, but must be retained long enough to allow individuals to access it if it has formed the basis of a decision that affects them.

Safeguards Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Use Use refers to the treatment and handling of personal information within an organization.

Related Privacy Links

For additional information and resources on privacy and related issues, refer to the Web sites listed below. These sites represent a sample of international perspectives, and contain additional links to a wealth of privacy information.

- **Office of the Information and Privacy Commissioner/Ontario**
  http://www.ipc.on.ca

- **Privacy Commissioner of Canada**
  http://www.privcom.gc.ca

- **Federal Trade Commission (United States of America)**
  http://www.ftc.gov

- **International Virtual Privacy Office**
  http://www.privacyservice.org

- **OECD – Information Security and Privacy**
  http://www.oecd.org/dsti/sti/it/secur/index.htm

- **Australian Privacy Commissioner**
  http://www.privacy.gov.au